Published and Copyright (c) 1999 - 2011
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1305 02/04/10

~ Egypt Goes Dark on Web ~ People Are Talking! ~ Firefox 4 Delayed!
~ New Canada Web Billing ~ Google: Bing A Copycat ~ Microsoft Is Riled!
~ Firefox Do Not Track! ~ Web Addresses Depleted ~ Aliases on Hotmail!

~ Chrome Is Uncrackable? ~ UK: Cyberspace Rulings ~ IE Patch and More!

-* Egypt Internet Back, Hacked! *-
-* The Internet Kill Switch That Isn't *-
-* China Gives Parents Control Over Gaming! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

The weather in the Northeast - and probably in many places throughout the country - is no longer bordering on the absurd. It's reached a point that is well beyond that now. Two more feet of snow this week, and more forecast for Saturday. Wow, maybe only 3-4 inches of snow and rain - a "flurry" compared to what we've been seeing week after week since since just after Christmas.

Sure, it's brutal for those of us who have to clear driveways and walkways, dig out mailboxes and various other areas around our homes. And yes, it's been difficult driving, or schools being closed for the kids. But now, because of so much snow, a "new" problem has become a very dangerous issue: roof collapses. According to tonight's early news, there have been reports of at least 92 roof collapses in Massachusetts in the past week alone. Too much snow, and a little melting, is causing ice jams and too much weight on may roofs throughout the area. Personally, the roof on my house has ice jams all the way around; and I've been trying to clear away some of the snow off of the various roof areas on my house. I even got a ladder out and climbed up onto the roof of my front porch to clear away the snow and break up some of the ice jams along my gutter. My wife got concerned for my safety (and stupidity?) and made me come down!

My concern is with no place for the water to go, and the weight of all of this snow, something bad could possibly occur - including the possibility of a collapse somewhere! With rain and snow forecast for tomorrow, that means additional weight. I don't know how much more the roof can manage, but I may try to clear away some more snow and break up some more ice - at least where I can without having to actually get up on a roof to do so. Unfortunately, however, there aren't a lot of places where I can safely set up a ladder to be able to reach some spots; there's just too much snow everywhere! I guess if I can reduce some of the weight on the roof and perhaps provide someplace for some water to run, I'll be better off than having done nothing to try and alleviate some of the problem. Do I even need to say that I'm sick of winter and snow?! Good luck to all of you, wherever you are and the weather issues that you're facing this winter!

Super Bowl prediction: Green Bay will lose a turnover, giving Pittsburgh the opportunity to score a field goal. That field goal will turn out to be the deciding factor for a Steelers victory, by three points!

Until next time...

=~=~=~=

->In This Week’s Gaming Section - China Gives Parents Control!
"""""""""""""""""""""""""""""""""

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

China Gives Parents Control of Kids’ Online Gaming

Chinese authorities have ordered online video game operators to allow parents to monitor their children’s playing sessions as part of a nationwide crackdown on the growing problem of Internet addiction.

The Ministry of Public Security was one of eight government departments that issued a joint notice on Monday ordering online gaming companies to comply with the new guidelines by March 1.

Upon proving their identity, parents will be able to put daily or weekly restrictions on their child’s game playing time, the notice said. They would also have the option of putting in place a total ban.

Some parents and experts however expressed doubts that the order would be effective.

"It’s unnecessary and it will prompt more rebelliousness from the children," Xie Guangji, the father of a 14-year-old boy in Cangzhou in northern Hebei province, was quoted as telling the China Daily newspaper.

Gu Jun, a sociologist at Shanghai University, said the order seemed unfeasible and a recipe for family conflicts.

"It’s a governmental gesture rather than an efficient solution," Gu told the newspaper.

The notice also spelled out that online game companies had a responsibility to help parents restrict "inappropriate" video game playing.

It urged game operators to employ special staff to assist with the project and to set up web pages and hotlines.

The document suggested children should spend less than two hours a week playing online games and should spend no more than 10 yuan ($1.50) on online games a month.

The number of teenage Internet addicts in China has risen to 33 million,

the China Daily reported, citing the Chinese Academy of Social Sciences, a government think-tank.

Concerns over Internet addiction have spurred a new industry, with unlicensed Internet treatment centres springing up around China.

Last year, two web "boot camp" instructors were sentenced to up to 10 years in prison after a 15-year-old was beaten to death at a treatment facility in the southern region of Guangxi.

At another rehabilitation centre in east China's Jiangsu province, 14 youths staged a mutiny in June, tying up their instructor and fleeing the facility over its tough military-like techniques, state media reported.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Last Internet Provider in Egypt Goes Dark

The last of Egypt's main Internet service providers, the Noor Group, has gone dark.

The Noor Group had remained online even after Egypt's four main Internet providers - Link Egypt, Vodafone/Raya, Telecom Egypt, Etisalat Misr - abruptly stopped shuttling Internet traffic into and out of the country Friday morning.

At about 11 p.m. local time Monday, the Noor Group became unreachable, said James Cowie, chief technology officer of Renesys, a security firm based in Manchester, N.H. Renesys monitors massive directories of "routes," or set paths that define how Web traffic moves from one place to another. The Noor Group's routes have disappeared, he said.

Cowie said engineers at the Noor Group and other service providers could quickly shut down the Internet by logging on to certain computers and changing a configuration file. The original Internet blackout on Friday took just 20 minutes to fully go into effect, he said.

Cell phone service was restored in Egypt starting Saturday but text messaging services have been disrupted as protests continue.

Google Inc., meanwhile, said that over the weekend it had developed a new service that will allow people in Egypt to post Twitter messages without an Internet connection. The so-called speak-to-tweet service was developed by engineers from Google, Twitter and SayNow, a company Google acquired last week.

With the service, which is already live, people in Egypt can post tweets by dialing an international telephone number and leaving a voicemail

message. The message is then sent out as a tweet with the hashtag (hash)egypt.

"We hope that this will go some way to helping people in Egypt stay connected at this very difficult time," Google said in a blog posting Monday.

Hackers Attack Egyptian Government Sites; Internet Back

Hacker activists started attacking Egyptian government websites on Wednesday, apparently taking them offline soon after the country restored Internet service.

An Internet forum run by a loose international group that calls itself "Anonymous" directed participants to attack the websites of the Egyptian Ministry of Information and the ruling National Democratic Party. Neither was accessible from New York on Wednesday afternoon.

In a Twitter post, the group claimed credit for taking down the ministry's website and said the group was motivated by a desire to support Egyptian protesters.

The same group rallied to support WikiLeaks in November and December, attacking websites of companies it saw as hampering the document-distribution site.

The Egyptian government cut off all Internet service in the country on Friday, then restored it early Wednesday.

One member of Anonymous, speaking on condition of anonymity because of the possibly illegal nature of its activities, said the number of participants in the attacks was much lower than it was in December. Thousands of young people then joined in attacks on such sites as MasterCard.com and Visa.com - in those cases because the payment processors declined to transfer money to WikiLeaks.

But because the Egyptian government websites are much easier to take down, the lower number of participants is still adequate, the member said.

The member said the weapon of choice for the hackers is the same as in December: a small program called Low Orbit Ion Cannon. It sends out a flood of fake traffic to a selected website, swamping it if it doesn't have enough capacity.

The Internet Kill Switch That Isn't

A cybersecurity proposal in the U.S. Congress, called an "Internet kill switch" plan by some critics, isn't exactly what that sounds like.

Plans by members of the U.S. Senate Homeland Security and Government Affairs Committee to reintroduce 2010's Protecting Cyberspace as a National Asset Act have led some critics to compare provisions in the bill to the Egyptian government's order to shut down all Internet access across

the country during recent protests.

But the Egypt comparison - and the term "Internet kill switch" - is a stretch. Still, some tech and civil liberties groups have questioned the powers the proposal would give the president.

The proposal, not yet introduced as a formal bill this year, would give the U.S. president the power to take emergency measures, including possibly quarantining or shutting down parts of the Internet, only when there's an "ongoing or imminent" cyberattack on the nation's critical infrastructure.

The bill would require the president to take the "least disruptive" measures necessary, and the emergency powers would expire after 120 days without congressional approval.

The proposal would prohibit the president from shutting down the Internet to silence free speech, said Leslie Phillips, communications director for Senator Joseph Lieberman, a Connecticut Independent and chairman of the Senate Homeland Security Committee.

"There is no relation at all between Senator Lieberman's bill to strengthen our nation's cyberdefenses and events taking place in Egypt," Phillips said. "The emergency Internet measures in the senator's bill are designed to ensure that our most critical infrastructure, our economy and our way of life - all of which rely on the Internet - are protected from destruction."

But critics say the proposal would give the president broad new authority over the Internet. The emergency powers language in the bill is ambiguous, said Gregory Nojeim, senior counsel at the Center for Democracy and Technology.

Backers of the proposal say it would limit the authority granted the president in section 706 of the Communications Act of 1934 to take over or shut down wire and radio communications in a time of war.

Whether that section of the 1934 act would apply to the Internet is "open to debate," Nojeim said. Beyond that, the 2010 bill would not have abolished that old presidential authority, he added.

"There are restrictions on the new [cybersecurity] authority, and they are important, but there should be no doubt that the bill does not limit the authority the president has, and instead expands it," he said. "If the intent was to limit the president's authority, the bill fails to do so."

It's unfair to suggest the bill would give the president the power to shut down the Internet to squelch dissent, but the additional authority is "not sufficiently defined," Nojeim added.

The comparisons to the Internet shutdown in Egypt grew loud enough that the three sponsors of the 2010 bill, Senators Joseph Lieberman, Maine Republican Susan Collins and Delaware Democrat Tom Carper issued a statement this week condemning the actions there.

"We would never sign on to legislation that authorized the president, or anyone else, to shut down the Internet," they said in the statement. "Emergency or no, the exercise of such broad authority would be an affront to our Constitution."

The three senators called the actions by the Egyptian President Hosni Mubarak "totally wrong."

"His actions were clearly designed to limit internal criticisms of his government," they said. "Our cybersecurity legislation is intended to protect the U.S. from external cyber attacks. Yet, some have suggested that our legislation would empower the president to deny U.S. citizens access to the Internet. Nothing could be further from the truth."

The senators' statement didn't comfort Free Press, a media reform and digital rights group.

"It's good to see the senators have heard the outcry from Americans troubled by this bill, but their promises that the bill won't give the president 'kill-switch' powers aren't very reassuring," Timothy Karr, campaign director for Free Press, said in a statement. "The devil is always in the details, and here the details suggest that this is a dangerous bill that threatens our free speech rights."

The proposal would give the president the authority to take emergency actions without congressional approval, Free Press said. The result is a concentration of power with the president, the group said.

"We understand that protecting Internet communications is a vital government interest, but we're troubled by the idea that the president could declare an emergency and shut down digital communications," Karr added. "In its current form, the legislation offers no clear means to check that power."

While the senators say the bill does not allow emergency actions in response to dissent, national security problems and political crises can become intertwined, added Heather Greenfield, a spokeswoman for the Computer and Communications Industry Association, a tech trade group.

"What governments do today in response to legitimate concerns can open the door to future abuses," she said.

Democracies should be models for Internet openness and freedom, she added. "CCIA doesn't want any government, or international body like the U.N., to expand their control over Internet operations," Greenfield said.

Firefox 'Do Not Track' Ready for Download Now

Adventuresome Firefox users who can't wait to try out the "do not track" feature can do so now by grabbing a "nightly build" of the browser. Nightly builds are for testing purposes only, Mozilla warns, and aren't as stable as beta releases.

Last week, Mozilla released details about a feature it intended to add to the upcoming version of its Firefox web browser, release 4.0, that would create a universal "opt-out" for net surfers who don't want to be tracked by Internet marketers. Today, Sid Stamm announced on his "extreme geekboy" blog that the first iteration of the feature has been incorporated into the latest nightly builds of the browser.

To enable the feature, open the preference pane in the software, select

the advanced tab and click the box labeled "Tell sites I do not want to be tracked."

After setting up "do not track," every time the browser makes a connection to download content, it will send a "don't track me" signal to the site. The syntax of that command has been changed slightly in this version of the feature compared to previous ones. It's now "DNT: 1". Previously, it was "X-Do-Not-Track."

Just because a browser has a "do not track" feature, though, doesn't mean a website will recognize it. "We do not anticipate that sites are looking for the signal yet, so you probably won't notice a difference as you browse the web," Stamm acknowledged.

That cooperation from both browser makers and website operators is required for "do not track" to work is seen by some as a major flaw in the system. As my colleague Tony Bradley pointed out last week:

"The problem with expecting cooperation from websites that are tracking Internet usage and gathering information on users' web habits is that most of those organizations are already aware that it is ethically questionable, and that the FTC is working to combat the practice, yet they choose to continue collecting the data anyway."

Outcry Mounts Over Canadian Internet Billing Ruling

Backed by a public outcry, Canadian opposition parties lined up on Tuesday to voice concerns about a regulatory decision that chokes off the ability of small independent Internet providers to offer unlimited downloading to their customers.

The regulator, the Canadian Radio-television and Telecommunications Commission (CRTC), gave major telecom carrier BCE Inc approval last week to charge wholesalers that use its network on the same usage-based billing (UBB) basis it uses to charge its customers, minus a 15 percent discount.

Major providers such as Bell, Shaw Communications and Rogers Communications charge customers extra if they download more than the monthly limits the big providers set, typically between 20 and 60 gigabytes.

Small providers often offer plans with 200 gigabyte ceilings, or even unlimited use.

At least one market participant and an individual citizen have appealed the regulator's decision.

One of the small providers, TekSavvy, will cut its usage ceiling to 25 gigabytes effective March 1, the date the CRTC ruling comes into force. On Tuesday, its website was festooned with links to groups opposing the pricing framework.

Citizen group Openmedia.ca said on Tuesday its "Stop The Meter" petition opposing usage-based billing had garnered more than 200,000 signatures, up from around 40,000 before the CRTC handed down its decision.

The opposition Liberal and New Democratic parties said the regulator’s decision limits competition and punishes consumers.

"We do not agree with the CRTC’s decision on usage-based billing, and we will bring the fight for an open and innovative Internet environment to Parliament," Liberal critic Marc Garneau said in a statement.

"Usage-based billing is squashing competition and hitting Canadian consumers in the pocketbook," said Charlie Angus of the New Democrats.

Another opponent of the pricing scheme is Netflix, whose launch of an online-only movie service in Canada in September spooked the incumbent providers.

Conservative Industry Minister Tony Clement said he was aware an appeal had been lodged and that the government would study the CRTC’s decision "to ensure that competition, innovation and consumers were all fairly considered".

Openmedia.ca’s national coordinator, Steve Anderson said Clement would have to do more than ask the CRTC to tinker with pricing.

"He must either overturn all the CRTC rulings that force pricing schemes on big telecom’s independent competitors, or at minimum have the CRTC revisit the entire premise of forced UBB pricing," he said.

BCE, the parent of telecom Bell Canada, and other telecom operators have spent heavily on infrastructure and are mandated to lease their networks to small providers to encourage competition.

Copycat? Google Says Bing Copies Search Results

Is Bing copying Google’s search results? Google says yes and Microsoft says no - and it’s stirring up plenty of drama in the search world this week.

Google offers sophisticated experiment results that it says proves Bing is using its search results. Google said it first noticed Bing’s alleged copycat behavior last summer and took a closer look over the following months. According to Google, URLs from Google search results would later appear in Bing with increasing frequency for all kinds of queries - even results Google considered mistakes from its algorithms.

"We created about 100 ’synthetic queries’ - queries that you would never expect a user to type, such as [hiybbprqag]," said Google Fellow Amit Singhal. "As a one-time experiment, for each synthetic query we inserted as Google’s top result a unique (real) web page which had nothing to do with the query."

Google then gave 20 of its engineers laptops with a fresh installation of Microsoft Windows running Internet Explorer 8 with Bing Toolbar installed. As part of the install process, Singhal said Google opted in to the Suggested Sites feature of IE8 and accepted the default options for the Bing Toolbar.

"We asked these engineers to enter the synthetic queries into the search box on the Google home page and click on the results - i.e., the

results we inserted," Singhal said. "We were surprised that within a couple weeks of starting this experiment, our inserted results started appearing in Bing."

Singhal said the experiment confirmed Google's suspicions that Bing is using some combination of Internet Explorer 8, which can send data to Microsoft via its Suggested Sites feature, and the Bing Toolbar, which can send data via Microsoft's Customer Experience Improvement Program, or possibly some other means to send data to Bing on what people search for on Google and the Google search results they get.

Microsoft quickly responded to Google's allegations. Harry Shum, corporate vice president for Bing, called the issue a spy-novelesque stunt to generate extreme outliers in tail query ranking.

"It was a creative tactic by a competitor, and we'll take it as a backhanded compliment," Shum said. "But it doesn't accurately portray how we use opt-in customer data as one of many inputs to help improve our user experience."

Shum went on to say that many companies across the Internet use collective intelligence to make their products better every day and defended Bing's "distinct approach to search."

So who's right? Is Bing all-out copying Google's search results? Or is Bing simply improving its search engine based on collective intelligence?

As Greg Sterling sees it, the verbal brawl marks a bitter public-relations turn in the intensifying competition between the two companies.

"Arguably Google did catch Bing doing something improper and copying selected Google results. But people also defend what Bing was doing as capturing 'public' user behavior and clicks and factoring that into its algorithm," Sterling said. "As it stands now, this isn't going to have much of an impact on consumers in the end, but among tech insiders it would appear to tarnish Bing's brand."

Microsoft Riled by Charge Bing Is A Copy Cat

A spat between Internet titans heated up with Microsoft angrily denying that Bing copies Google's search results and the world's top online search engine adamant it has proof.

Microsoft senior vice president Yusuf Mehdi went on the offensive in a blog post that accused Google of tricking Bing with a "honeypot attack" too sweet to resist.

"In simple terms, Google's 'experiment' was rigged to manipulate Bing search results through a type of attack also known as 'click fraud,'" Mehdi said.

"That's right, the same type of attack employed by spammers on the Web to trick consumers and produce bogus search results."

Google held firm that it conducted a simple, honest experiment that showed Bing copied its search results and that rather than gripe about

getting caught it should simply stop doing it.

"Some Bing results increasingly look like an incomplete, stale version of Google results - a cheap imitation," said Amit Singhal, one of the company’s search engineers, on Google’s official blog.

Google had noted that in the summer of 2010 Bing did not return any results for a misspelled search for the surgical eye procedure "tarsorrhaphy."

"Later in the summer, Bing started returning our first result to their users without offering the spell correction," Singhal said. "This was very strange."

The experiment was repeated with nonsensical searches, including "hiybbprqag," "delhipublicschool40 chdjob," and "juegosdeben1ogrande," which Google had designed to link to a single unrelated result.

Google engineers used their company’s search engine and Microsoft’s Internet Explorer web browsing software to search on the fabricated terms that generated orchestrated results.

Within weeks, Bing offered the same results for searches on the made-up terms, according to Singhal.

Google equated the experiment to releasing intentionally false information and following its trail.

"We do not copy results from any of our competitors," Mehdi said. "Period.

"We have some of the best minds in the world at work on search quality and relevance, and for a competitor to accuse any one of these people of such activity is just insulting," he continued.

Microsoft argued that search feedback from users of Internet Explorer is "one of more than 1,000 signals" taken into account by its formula to match online queries with results.

Bing gets information from users who agree to share anonymous data "as they navigate the web in order to help us improve the experience for all users."

Google found it suspicious that a fictional search term and fabricated results popped into Bing if they were just one signal in a sea of more than 1,000 signals considered by Microsoft’s ranking software.

"However you define copying, the bottom line is, these Bing results came directly from Google," Singhal said in a blog post detailing the sting operation.

"To those who have asked what we want out of all this, the answer is simple: we’d like for this practice to stop."

Bing corporate vice president Harry Shum dismissed Google’s experiment as "a spy-novelesque stunt."

"It doesn’t accurately portray how we use opt-in customer data as one of many inputs to help improve our user experience," Shum said.

"We all learn from our collective customers, and we all should," Shum

said.

Firefox 4 Delayed Again, 12th Beta Planned

A week after releasing its tenth beta of Firefox 4, the open-source browser project's release manager, Christian Legnitto this week announced a new beta plan, which will include a 12th beta.

Previously Legnitto had written that there were no plans for a beta 12 for Mozilla's the next major desktop Web browser.

Beta 11 is finished, and the Firefox planning page on the Mozilla wiki states that the team is "still working on an ETA for releasing it to our beta audience, likely early next week." That page also mentions Beta 12 as having "a small enough list of bugs that it's plausible it will be the last beta, though we're not locking that up, since some of the plugin work needs to crystallize before we can assess timing risk."

Many of the holdbacks seem to be related to Flash and Hotmail. Beta versions of Firefox come with a reporting plug-in that lets testers send comments to the developers. The comments are viewable at the Firefox Input Dashboard page, and nearly 3,700 of these have to do with Hotmail constantly refreshing. Over 1,800 mention Flash, but many involved problems with basic browser functions, such as the new Panorama tab-previewing feature, copy and paste, and password saving.

The ability for anyone to view these comments, along with Legnitto's post gives an inside view into the open-source development process. "If anything is even slightly risky," says the release manager to his developers, "please hold off a day until we branch for beta 11 before landing on mozilla-central. We will not close mozilla-central and instead trust developers to act responsibly with risk."

Firefox 4 will be a major upgrade to the browser alternative to products from billion-dollar corporations, such as Internet Explorer, Google Chrome, and Apple Safari. It will feature a revamped plug-in architecture called JetPack, a redesigned minimalist interface, faster JavaScript performance, and greater support for HTML5, including Google's WebM HTML5 video format.

A schedule on Mozilla's wiki for Firefox 4 Beta releases listed Beta 11 as "Asap in the week of January 31" while the launch of the Firefox 4 Release Candidate (RC) was still vaguely listed as "Early 2011."

Microsoft 'Love' Means Massive Reboots for IE Patch

Microsoft announced 12 bulletins for February's Patch Tuesday. Three of the bulletins are critical and include updates to address recently disclosed flaws in Internet Explorer and Windows.

Beyond the three critical bulletins, nine are rated important, addressing issues in Microsoft Windows, Internet Explorer, Microsoft Office, Visual Studio, and IIS.

February’s Patch Tuesday release comes after only two security bulletins addressing three vulnerabilities were issued in January. But January’s light Patch Tuesday skipped some known vulnerabilities, including the recursive style-sheet load bug in IE.

"These vulnerabilities have seen limited exploits in the wild, so applying the update is highly recommended," said Wolfgang Kandek, CTO at Qualys. "In addition, the lower-rated flaw in the FTP service is addressed with an update to the IIS server."

The remaining updates address flaws in Windows, Office and the development platform Visual Studio. Kandek said all versions of Windows, starting with Windows XP SP3 up to the latest versions of Windows 7 and Windows Server 2008 R2, are affected. The Office bulletin, however is limited to a relatively small footprint: The Visio versions 2002, 2003 and 2007.

"The recent MHTML issue in Windows and Internet Explorer will not be addressed in this update," Kandek said. "The work-around suggested by Microsoft in Advisory 2501696 continues to be the recommended way of mitigating this attack vector."

The vulnerability exists due to the way MHTML interprets MIME-formatted requests for content blocks within a document. Microsoft said it’s possible under certain conditions for this vulnerability to allow an attacker to inject a client-side script in the response of a web request run in the context of Internet Explorer.

Technical details aside, Paul Henry, forensic and security analyst at Lumension, said it looks like IT admins might be finally getting a patch for Internet Explorer this month. That means 900 million people will be sharing the love for Microsoft this Patch Tuesday.

"Last month, we were waiting for the IE patch that never came, and this month we get to celebrate the national day of love by all of us simultaneously rebooting our PCs," Henry said. "Not only do we expect to see a lot of noise around the IE patch, this Patch Tuesday we will see another massive round of patches. In the 12 bulletins released today, six are remote-code executable."

Will history repeat itself with this massive reboot?

Experience tells Henry that reboots of this magnitude have been known to upset services and applications, so it’s possible IT admins will see similar problems to what was encountered in 2007 when a large Microsoft patch that required a reboot crippled applications -- Skype in particular.

"Although Microsoft appears to be doing a bit of spring cleaning this Patch Tuesday with a lot of regular ’run of the mill’ stuff, it can’t be emphasized enough that this will be a massive simultaneous reboot and historically, we’ve seen services greatly impacted when such a huge number of machines require reboots," Henry said.

Microsoft Hides Your Email Address via Hotmail Aliases

Microsoft said Thursday that it has enabled aliases on Hotmail accounts, allowing people to create temporary email addresses.

Users who create an alias can route emails to that alias to a separate folder, which can then be managed separately. For example, email sent to "markthereporter@hotmail.com" will be sent to a private folder that will be accessible from my main Hotmail account.

Beginning today, users can add up to five email aliases per year to each account, up to a maximum of fifteen.

So far, the alias feature is exclusive to Microsoft; Google hasn't added it to its Gmail mail system.

Microsoft positioned the alias feature as the email equivalent of a one-time credit card number that can be used on a dodgy shopping site. "Let's say you're in the market for a new car," Dharmesh Mehta wrote in a blog post. "There are a bunch of websites that will email you price quotes, sales alerts, etc. During your car search, these messages are helpful, but once you're done, they become clutter that can be difficult to stop. By using an alias on these websites instead of your main email address, you can avoid this. And when you're done, just turn the alias off, ensuring future unwanted messages that are sent to that alias don't land in your inbox."

Gmail does allow users to add a "+" to their email addresses to create a sort of alias; addressing emails to "johnqpublic101+home@gmail.com" will route the email to the johnqpublic101 inbox, add indicative stars to them, or route them to the trash. But Mehta also argued that such methods are detectable, including by humans.

Hotmail also allows a user to access email stored in a non-Microsoft account, pulling the information via POP, rather than IMAP.

In December, Hotmail added sandboxing to its email accounts, which can protect the system from malicious scripts. The "Active Views" technology isolates JavaScript. Microsoft also added additional security verification technology, using cell phones and a trusted PC. All are followons to a revamped Hotmail client that Microsoft began rolling out last summer.

Internet Addresses Depletion Reflects Wired World

Thirty years after the first Internet addresses were created, the supply of addresses officially ran dry on Thursday.

But don't panic. The transition to a new version of addresses is already well under way and, for most people, should occur without even being noticed.

At a special ceremony in Miami on Thursday, the organization that oversees the global allocation of Internet addresses distributed the last batch of so-called IPv4 addresses, underscoring the extent to which the Web has become an integral and pervasive part of modern life.

Every computer, smartphone and back-end Web server requires an IP address - a unique string of numbers identifying a particular device - in order to be connected to the Internet. The explosion of Web-connected gadgets, and the popularity of websites from Google Inc to Facebook, means that the world has now bumped up against the limit of roughly 4 billion IP

addresses that are possible with the IPv4 standard introduced in 1981.

The solution is IPv6, a new standard for Internet addresses that should provide a lot more room for growth: There are 340 undecillion IPv6 addresses available. That’s 340 trillion, trillion, trillion addresses.

"If all the space of IPv4 were to be sized and compared to a golf ball, a similar-sized comparison for IPv6 would be the size of the sun," said John Curran, the chief executive officer of the American Registry for Internet Numbers, one of five nonprofit organizations that manage Internet addresses for particular regions of the world.

Just in case you’re worried, Curran added that "we don’t ever intend to see another transition."

For companies with websites, the transition to IPv6 means configuring their computer equipment to support the new standard rather than upgrading hardware, Curran said. Those that don’t could see the performance of their sites slowed down, and potentially cut off to some users in the future.

Laptops, smartphones and other Web-connected gadgets, as well as Web browsers, already support IPv6, though Curran notes that according to some estimates less than 1 percent of Internet users may not have their equipment configured properly and will need to adjust their settings in the months ahead, as websites increasingly adopt the new standard.

Google Gambles $20K that Chrome Can’t be Cracked

Google is so confident that its Chrome Web browser can’t be hacked that it is willing to put $20,000 cash and a Chrome CR-48 notebook on the line to prove it. At the 2011 Pwn2Own contest, held in conjunction with the CanSecWest security conference in Vancouver next month, Google will put its money where its proverbial mouth is.

Google’s use of Chrome as the name of both its browser and its OS is creating some confusion. There are some false reports that Google is offering the bounty for successfully cracking its Chrome OS-based CR-48 notebook. The Google CR-48 notebook will be awarded along with the $20,000 for a successful attack against the Chrome Web browser, but the Pwn2Own info clearly states that the notebook is merely a prize. There will be no attacks mounted against the Chrome OS, and the target Chrome Web browser will actually be running on the latest 64-bit release of either Windows 7 or Mac OS X.

The Chrome Web browser is the only participating browser with built-in sandbox protection. The sandbox segregates untrusted or potentially malicious scripts so they are unable to impact the core browser, or the underlying PC. Because of the sandbox, it will take some extra effort for an attack against the Chrome Web browser to be considered a success.

According to posted details about the Pwn2Own contest, a successful attack against Chrome will be measured over a few days. "On day 1, Google will offer $20,000 USD and the CR-48 if a contestant can pop the browser and escape the sandbox using vulnerabilities purely present in Google-written code. If competitors are unsuccessful, on day 2 and 3 the ZDI will offer $10,000 USD for a sandbox escape in non-Google code and Google will offer

$10,000 USD for the Chrome bug. Either way, plugins other than the built-in PDF support are out of scope."

Google’s $20k award is the largest ever offered at the annual Pwn2Own contest, and also the first time that a Web browser vendor has stepped up to contribute to the Pwn2Own cash pool. Perhaps the bravado is inspired by the fact that this will be the third year that Chrome will be targeted, yet it has remained un-cracked in years past.

Compare that to Apple’s Safari Web browser, which is perennially cracked in minutes - if not seconds. But, even Firefox and Internet Explorer have fallen prey to Pwn2Own attacks. Only Chrome remains unscathed...so far. We’ll see if $20,000 is enough incentive for an enterprising hacker to find a crack in its armor.

Britain Wants International Rules on Cyberspace

Britain, worried about a growing threat from cyber espionage and cyber crime, offered Friday to host an international conference to tackle such issues.

Foreign Secretary William Hague, speaking at a security conference in Germany, revealed details of recent attacks on British government and defense industry computers to underline the threat from cyber spying.

He also cited how the Egyptian government had tried to shut down the Internet, mobile phone networks and broadcasters during mass protests against the rule of President Hosni Mubarak.

He said cyber security was on the agenda of some 30 international organizations, but the debate lacked focus.

"We believe there is a need for a more comprehensive, structured dialogue to begin to build consensus among like-minded countries and to lay the basis for agreement on a set of standards on how countries should act in cyberspace," he said.

"The UK is prepared to host an international conference later this year to discuss norms of acceptable behavior in cyberspace," he added in the speech, the text of which was released in London.

Cyberspace had opened up new channels for hostile governments to try to steal secrets and created new means of repression, "enabling undemocratic governments to violate the human rights of their citizens," Hague said.

"It has promoted fears of future ’cyber war’," he said.

International rules on the use of cyberspace should be based on principles including respect for individual privacy, protection of intellectual property and a collective effort to tackle the threat from criminals acting online, he added.

Hague described several recent attacks on British government or defense contractors’ computer systems.

Last year, a malicious file posing as a report on a nuclear Trident

missile was sent to a defense contractor by someone masquerading as an employee of another defense firm, Hague said.

"The email was detected and blocked, but its purpose was undoubtedly to steal information relating to sensitive defense projects," he said.

Britain's eight-month-old coalition government has produced a new national security strategy which ranks cyber attack and cyber crime as a high priority risk. It is spending 650 million pounds ($1.05 billion) on a national cyber security program.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.